基于区块链的可扩展电子取证模型研究 *

孙靖超

(中国人民公安大学 侦查与刑事科学技术学院, 北京 100032)

摘　要：区块链技术可以使电子证据摆脱中心化机构的制约，提高存证效率和可信性。针对现有区块链在电子取证方面存在的可扩展性和可用性较差的问题，设计了一种基于委托权益证明-实用拜占庭容错的链上链下结合的区块链电子取证模型。首先通过委托权益证明的方法投票选出区块生产者，然后仅在区块生产者之间运用实用拜占庭机制进行同步，针对区块链技术本身不适于存储大容量数据的特点，采用链上链下结合的方式进行数据存储。对所提模型进行了安全性和效率分析，证明所提模型能同时满足安全、性能的需求，可以很好的支持电子取证。

关键词：区块链；电子证据；电子取证；共识算法

中图分类号：TP311;TP393　　doi: 10.19734/j.issn.1001-3695.2020.03.0032

Research on scalable digital forensics model based on blockchain

Sun Jingchao

(*School of Criminal Investigation & Forensics Science*, *People's Public Security University of China*, *Beijing* 100032, *China*)

Abstract: With the decentralized anti-tampering feature of blockchain technology, digital evidence is being freed from the constraints of centralized institutions, and the efficiency and credibility of depositing evidence has been improved. In order to solve the shortcomings of weak scalability and availability, a parellel storage blockchain digital forensics model based on the combination entrusted equity and practical Byzantine fault tolerance is proposed. Firstly, the block producers are selected by the method of Delegated Proof of Stake, and then the Practical Byzantine Fault Tolerance mechanism is used to synchronize the block producers. In view of the characteristics that the block chain technology itself is not suitable for storing large capacity data, a combination of blockchain and off-chain storage is applied to overcome this problem. The safety and efficiency analysis of the proposed model proves that the proposed model can meet the requirements of safety and performance at the same time, and can serve digital forensics feature well.

Key words: blockchain; digital evidence; digital forensics; consensus algorithm

0　引言

电子证据是以电子计算机技术的发展为前提条件产生的新型证据。对电子证据概念的理解学界众说纷纭，但毋庸置疑的是，这种新型证据带来的影响巨大，渗透到了生活的许多角落[1]。电子证据本身具有的易窜改特性阻碍了其在实务界的具体应用和理论界的深入研究[2]并限制了其证据能力[3]。中本聪于 2008 年[4]构建了一种去中心化的电子货币—比特币，论文中对其去中心化、不可窜改、可追溯的底层技术区块链进行了详细阐述。区块链技术引起了各界的高度重视[5][6]，如今在网络舆情[7]、信息保护预测[8]、开放资源获取[9]等各个领域均有丰富的研究成果。学界当前针对电子证据的研究多集中于其形成与真实性认定[10, 11]、客观化采信[12]及认证规范[13]领域，对将其应用于构建电子取证模型中也取得了一定成果。黄晓芳等[14]提出了一种基于区块链的云计算电子取证模型，该模型基于 Merkle Tree 的证据保全及改进的共识算法，降低了区块产生时间。侯义斌等[15]提出了一种完整的基于区块链的电子取证系统，并描述了一种对电子证据的批量打包方式以提高存证效率。Cebe 等[16]构建了一种基于车联网取证的区块链基础设施，为事故调查提供全面的电子证据服务。Bonomi 等[17]构建了一种基于区块链的物证监管链，确保了所收集证据的可审计完整性和所有者的可追溯性。Ryu 等[18]本文提出了一种基于区块链的物联网环境数字取证框架，以解决物联网环境的异质性和分布特征以及现有取证调查的集中化问题。

如今利用区块链在不同应用场景下的电子取证方面的应用已取得了一定成果，但是在共识方法的选择上多采用了拜占庭容错算法，随着节点数的增多，通信成本会极具增加，影响了其在用户和交易数量方面的可扩展性和系统可用性。为了解决前人工作的不足，本文设计了一种基于委托权益证明-实用拜占庭容错的链上链下结合的区块链电子取证模型。首先通过委托权益证明的方法投票选出区块生产者，然后仅在区块生产者之间运用实用拜占庭机制进行同步，并采用链上链下结合的方式进行数据存储以解决区块链技术本身不适于存储大容量数据的问题。

1　相关理论

1.1　区块链技术

区块链技术在对等网络中实现了分布式存储的复制账本，该技术最初用于比特币加密货币。区块链由一系列包含交易记录的块组成，块内的事务按时间顺序排序。造块节点在接收到足够多的交易后会将其打包创建新的区块，一旦打包完成，便开始共识过程，以说服其他节点将其包含在区块链中。区块链用到了密码学中的数字哈希和签名技术，所有交易内容都是公开的，包括交易地址和具体内容。

1.2　共识机制

区块链的核心组成要素便是共识机制。如比特币的共识机制是工作量证明，通过解决哈希难题的形式来获得造块权。

收稿日期：2020-03-04；**修回日期：**2020-04-20　**基金项目：**中国人民公安大学 2020 年基本科研业务费科研机构项目(2020JKF209)；中国人民公安大学 2019 年基本科研业务费科研机构项目(2019JFK206)

作者简介：孙靖超(1993-)，男，山东烟台人，博士研究生，主要研究方向为侦查学(kenniyaligen@163.com).

此种共识机制在链上带来了显着的安全性(可承受多达 50%的节点是恶意的)，但是却以耗费巨大的计算量和时间成本为代价。共识机制在现阶段已取得了很大发展，以下是几种在区块链中主流的共识方案。

工作量证明(PoW，Proof of Work)：在 PoW 中，节点需要通过解决数学难题来达成共识。解决该数学难题不存在计算捷径，只能通过穷举的形式以得到符合要求的散列结果。涉及并依赖 PoW 共识机制的区块链具有交易确认慢、资源消耗高等问题。

权益证明(PoS，Proof of Stake)：PoW 的最常见替代方法是权益证明(PoS)。在 PoS 中，创造新区块的权利取决于谁拥有更多的加密货币，其中确定性算法根据每个人拥有的货币量来选择节点。因此，矿工们无须耗费高昂的计算资源来创建区块，矿工被选择创建一个区块的可能性大小取决于该矿工在系统中拥有的货币比例。

委托权益证明(DPoS，Delegated Proof of Stake)：委托权益证明(DPoS)是 PoS 的一种变体，在委托权益证明中，节点投票选择见证人。见证人是指通过投票的方式被选择出以验证交易的节点，每个节点可以都为其信任的见证人投票，投票权力的大小根据每个投票人所持股份数量来决定。顶层的见证人负责验证交易并为这些交易创建区块，在完成职责的同时可以获得一定收益。委托权益证明被设计为基于民主投票的实现方法，旨在通过使用投票和选举过程来保护区块链免受集中化制约和恶意使用。使用委托权益证明机制的加密货币有 Lisk，Steem，EOS 和 BitShares。

实用拜占庭容错(PBFT，Practical Byzantine Fault Tolerance)：实用拜占庭式容错是一种可以容忍拜占庭式错误的算法，在分布式系统中具有较低的算法复杂度和不错的实用性，可以在包含拜占庭式故障的异步环境中工作。该算法可以保证当高达三分之一的参与者受到损害时分布式系统仍具有可用性。

2 取证模型构建

2.1 链上链下结合的电子取证模型

区块链的电子证据模型如图 1 所示。

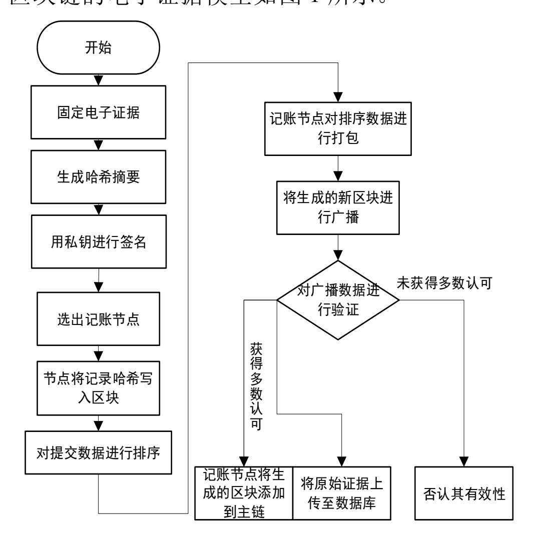


图 1 链上链下结合的电子取证模型

Fig. 1 Digital forensics model based on the combination of blockchain and off-chain storage

具体步骤如下：

a) 采用取证技术固定电子证据并记录时间和地理位置信息。

b) 对所收集的电子数据用公钥产生哈希摘要。

c) 用私钥对生成的哈希摘要、记录时间及位置信息进行签名。

d) 通过共识算法选出记账节点。

e) 选出的记账节点根据区块大小、交易等待时间等多种因素对数据进行综合排序。

f) 记账节点将排好顺序的数据打包到新区块之中。

g) 记账节点对生成的新区块进行广播。

h) 代表或矿工节点对广播区块数据的正确性进行验证，如获得多数认可，记账节点将生成的区块添加到主链并将原始数据上传至数据库，如未获得多数许可，则否认其有效性。

采用链上和链下相结合的方式进行存储的原因有二。首先，由于区块链技术的自身限制，证据可能太大而无法有效地存储在区块链中。其次，也是最重要的是，如果证据存储在区块链中，则区块链网络中的每个节点都可以进行访问，而现实情况中只应允许授权节点获取证据。因此，模型仅在区块链中存储证据哈希。

具体的证据存储在证据数据库中。证据数据库是一个普通的数据库或文件存储库，考虑到电子数据的多样性，宜采用非关系型数据库。原始数字证据与标志符 ID 一起存储在该标志符中，标志符 ID 作为证据的哈希值和随机数获得，以确保 ID 的唯一性。该数据库是分布式的，并且由受信任的实体管理。

证据日志存储在区块链中。证据日志通过区块链技术实现，并为每个证据存储其 ID，哈希摘要、记录时间、位置信息，描述，提交者(创建者)的身份以及所有者的完整历史(包括当前时间)。尽管证据本身未存储在区块链中，但只要使用健壮的密码哈希函数生成证据，ID 即可验证证据未被窜改。

网络可以分解为两组节点分别为验证者节点和轻量级节点。验证者节点主要具有存储区块链的副本，验证交易，创建，提议并向链中添加块(即参加共识协议)的功能。这一类节点必须在被许可的区块链中以验证者的身份进行预防性授权。轻量级节点可以看做是链的客户端，因为它们仅发出事务，并且需要依赖验证程序来添加和验证其事务。

2.2 基于委托权益证明-实用拜占庭容错的取证算法设计

委托权益证明的原理是让持有股权的节点投票选举区块创建者。这种投票方式使利益相关者将创建区块的权利赋予他们支持的代表，而不是自己创建区块。图 2 显示了取证模型造块节点算法流程。如图 2 所示，如果选出的代表无法正常生成区块，则将其解雇，利益相关者将选择新的节点来替换它们。委托权益证明充分利用股东的投票权，以公正，民主的方式达成共识。

a) 股权节点进行投票，高票节点成为代表节点。

b) 代表节点收集数据，将数据进行打包，进行造块。

c) 如果在给定时间内造块成功，则广播给其他节点进行验证，否则解雇该代表节点。

代表节点有很多义务，如果代表节点不称职或宕机，其他节点可以撤销选票，使其失去代表资格，每一个周期都会重新统计投票排名，在选出得票最高的几个代表节点中，系统先打乱顺序，然后依次产生区块，代表节点完成职责后可以领取奖励，每一个持币用户都有投票和竞选资格，投票能力大小和其所持币量以及持币时间有关，通过选票投出的代表节点去完成打包交易，既保证了选举效率又实现了去中心化。

在委托权益证明中，利益相关者选择见证人，见证人负责为区块链生成和添加区块。为见证人投票是一个连续的过程，声誉评分系统的存在可以帮助利益相关者更好地评估见证人素质。在分配的时间未能生成区块会导致见证人被跳过，并对其声誉产生负面影响，因此见证人有动力以最高标准履行职责，否则就有失去职位的风险。

取证模型造块节点算法仅确定谁和何时可以将块发送到

根链。在块进入根链之前，还需要知道是否有可能做到这一点并在所有验证者之间达成共识，为此期望将实用拜占庭容错算法引入取证模型节点验证过程中。

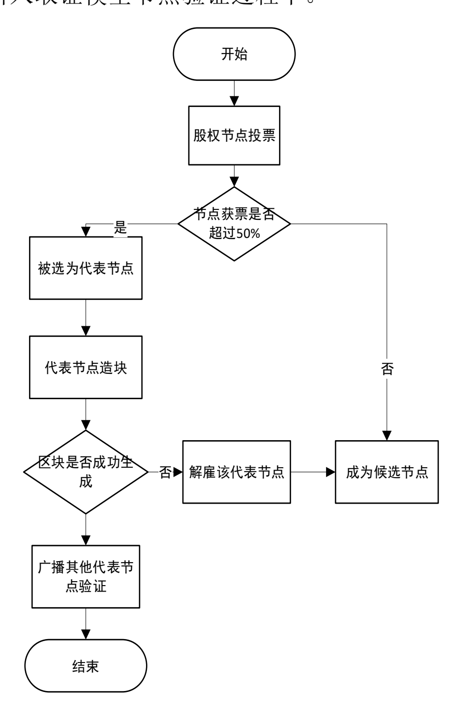


图 2　取证模型造块节点算法流程图

Fig. 2　Flowchart of node constructing algorithm of forensics model

实用拜占庭容错算法包含五个阶段：请求阶段，预准备阶段，预备准备，确认阶段和答复阶段。

图 3 描述了实用拜占庭容错算法的工作方式。节点 0 为主节点，节点 3 为故障节点。主节点将客户端发送的消息转发给其他三个节点，在节点 3 崩溃的情况下，一条消息将经历五个阶段以在节点间达成共识，在客户端收到节点回复后一轮流程结束。实用拜占庭容错算法保证节点保持共同状态，并在每一轮共识中采取一致的行动。实用拜占庭容错算法实现了强一致性的目标，因此它是绝对最终的共识协议。

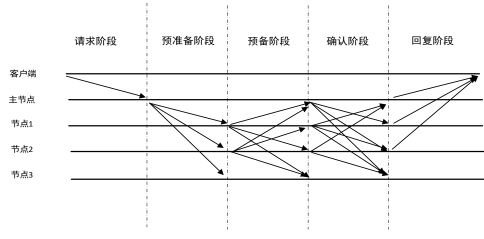


图 3　实用拜占庭容错算法流程图

Fig. 3　Flowchart of practical byzantine fault tolerance algorithm

根据以上原理，设计了取证模型节点同步算法，算法的具体工作流程如图 4 所示。

1) 客户端 A 通过向主服务器发送 $<REQUEST,o,t,c>_{\sigma_c}$ 消息来请求状态机操作 B 的执行。o 为请求执行的操作，时间戳记 t 用于确保执行一次客户请求的，c 请求的时间戳是完全有序的，因此以后的请求比以前的请求具有更高的时间戳。σ_c 为客户端签名。

2) 选出的主节点对请求进行接受。

3) 主节点对客户端发送的消息进行验证，验证客户端消息签名是否正确，如非法，则丢弃该请求，如合法，则对请求分配编号。

4) 打包预准备消息并签名，格式为 $<PRE-PREPARE,v,n,m>_{\sigma_p}$，其中 v 表示发送消息的视图编号，n 为主节点分配的消息编号，m 表示消息内容，σ_p 代表主节点签名。

5) 主节点将打包好的预准备消息广播给其他副本节点。

6) 副本节点对收到主节点广播的消息进行验证，验证主节点消息签名是否正确，n 是否在规定区间，是否接受过同一视图下同一序号的不同请求，如非法，则丢弃该请求，如合法，则进行下一步骤。

7) 各副本节点打包准备消息并签名，格式为 $<PREPARE,v,n,d,i>_{\sigma_i}$，其中 v 表示发送消息的视图编号，n 为主节点分配的消息编号，d 为消息摘要，i 为副本节点编号，σ_i 表示节点 i 的签名信息。

8) 各副本节点向其他节点包括主节点发送该消息。

9) 各节点对收到的准备消息进行验证，验证副本节点签名是否正确，n 是否在规定区间，是否接受过同一视图下同一序号的不同请求，如非法，则丢弃该请求，如合法，则记录该请求。

10) 当副本节点累计收到 $2f$ 个不同节点的合法准备消息，打包确认消息并签名，格式为 $<COMMIT,v,n,d,i>_{\sigma_i}$，其中 v 表示发送消息的视图编号，n 为主节点分配的消息编号，d 为消息摘要，i 为副本节点编号，σ_i 表示节点 i 的签名信息。

11) 各副本节点向其他节点包括主节点发送确认消息。

12) 各节点对收到的确认消息进行验证，验证副本节点签名是否正确，n 是否在规定区间，v 是否正确，确认消息和准备消息的识图、序号和签名是否相同，如非法，则丢弃该请求，如合法，则记录该请求。

13) 当副本节点累计收到 $2f+1$ 个不同节点的合法确认消息，运行客户端请求。

14) 打包回复消息并签名，格式为 $<REPLY,v,t,c,i,r>_{\sigma_i}$，$v$ 是当前视图号，t 是相应请求的时间戳，i 是副本号，r 是执行所请求操作的结果，σ_i 表示节点 i 的签名信息。

15) 各副本节点客户端发送回复消息。

16) 客户端收到的准备消息进行验证，验证副本节点签名是否正确，如非法，则丢弃该请求，如合法，则记录该请求。

17) 当副本节点累计收到 $f+1$ 个不同节点的合法确认消息，则确认结果有效，否则广播请求到所有副本。

18) 客户端向副本发送执行操作的请求，所有无故障的副本以相同的顺序执行相同的操作。由于副本是确定性的，并且以相同的状态开始，因此所有无故障的副本都会为每个操作发送具有相同结果的回复。客户端接收到来自不同副本的 f+1 个相同结果的回复，则结果有效。

实用拜占庭容错算法基于复制状态机方法(State Machine Replication)，状态机在分布式系统中的不同节点之间复制，每个副本都维护服务状态并实现服务操作，用 R 表示副本集，假设 $R=3f+1$，其中 f 是可能有故障的最大副本数。状态机复制中的难题是如何确保无故障的副本以相同的顺序执行相同的请求。实用拜占庭容错算法使用了主节点备份(primary-backup)技术进行排序，在主备份机制中，副本在一系列称为视图(view)的配置中移动。在视图中，一个副本是主节点(primary)，其他副本是备份(backup)，其中主节点副本通过 $p=v \bmod r$ 选出，其中 p 为节点序号，v 是视图编号。主节点选择执行客户端请求的操作的顺序，它为每个请求分配一个序列号，然后将此分配发送给备份副本。主节点可能会出现各种问题，如它可能将相同的序列号分配给不同的请求、停止分配序列号，或者在请求序列号之间留下空白。因此，当前主节点出现故障时，备份副本将检查由主节点分配的序列号，并触发视图更改(view-change)以选择新的主节点。

3　安全性与效率分析

3.1　安全性分析

通过假设以下威胁场景对所提模型的安全性进行分析。

场景 1　存在恶意节点，并形成少数分叉。在正常操作下，块生产者在一定时间间隔轮流产生区块。在少数恶意节点(少于总数 1/3)存在的情况下，恶意节点产生区块的速度将慢于诚实节点产生的区块速度，诚实的多数节点生产的链将永远比少数链更长，根据最长链原则，恶意节点产生的少数分叉将不被认可。

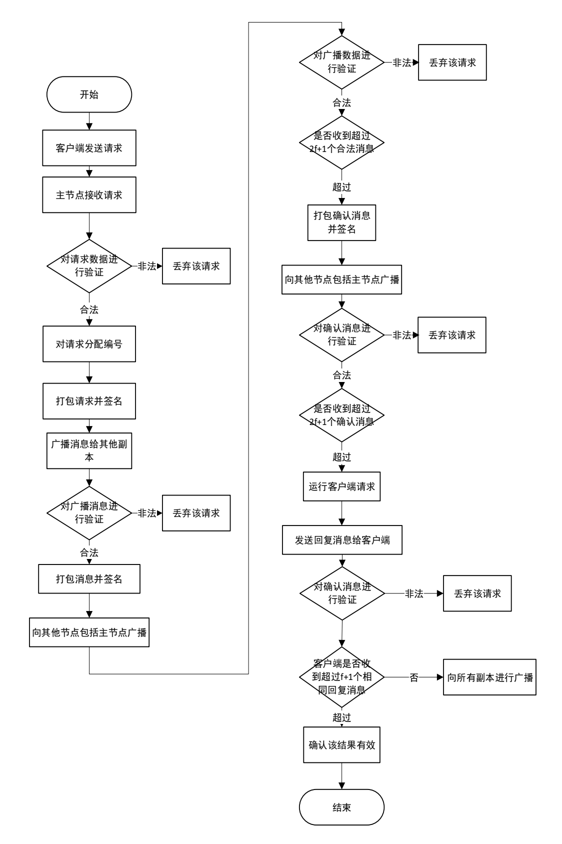


图 4　取证模型节点同步算法流程图

Fig. 4　Flowchart of node synchronization algorithm of forensics model

场景 2　节点产生重复区块。一种情况是少数离线节点可能尝试生产自己的分叉链，但是因为少数节点产生的分叉将比多数节点产生的链短，不会被主流节点接受。还有一种情况是在线节点产生区块时可能在其负责时序上产生了两个或更多的替代块，在这种情境下，下一个调度的生产者可以选择从其产生的任何备选方案中构建择一延伸，不会影响最长链的构建，因此尝试产生多少替代块并不重要。

场景 3　网络碎片化。这种情形多发生在网络连通性异常的情况下，该情形下最长的链将由最多少数节点产生。恢复网络连接后，较小的少数群体自然会切换到最长的链，并且将恢复明确的共识。在网络异常时，可能有两个分叉的长度相同，在这种情况下，较小的分支在重新加入网络时将打破平局。区块生产者总量为奇数，因此不可能长期维持平局，同时区块生产者混排将使生产顺序随机化，以确保即使两个分叉具有相同数量的生产者，这些分叉也会以不同的长度增长。

场景 4　多数生产者合谋。如果大多数生产者合谋，那么他们可以很多分叉，每个分叉都在多数票确认的情况下增长。但在这种情况下，最后一个不可逆块算法将使其中一条分叉恢复为最长链，即最长链仍由少数诚实节点决定。多数生产者合谋的情况不会持续很长时间，因为利益相关者最终会投票决定取代这些腐败节点。

场景 5　长程攻击。长程攻击指攻击者在短时间内造出一条长于主链的伪链。这种攻击在以股权为证明的共识方法中可能会发生，但在委托权益证明中，当用户签署交易时是基于对多个块认识(perception)，孤立分叉上的区块因未经过利益相关者的确认将不被认可从而无法替代主链。

场景 6　双花攻击。双花攻击的发生场景较多，如发生通信故障区块链进行重组时发现了之前不被包含的交易，就有可能发生双花攻击。模型中使用的委托权益证明算法能够监测网络的健康状况，能够及时发现见证人的异常情况，能及时封锁时立即发现通信中的任何损失，因此可以很大程度上避免双花攻击。

3.2　效率分析

3.2.1 共识等待时间

假设网络中总节点数为 N，消息传播采用流言算法，则需要传播的消息数量为 N^2，可以通过公式(1)来估算共识等待时间，即在验证者之间传播块 b 所需的时间。

$$latency_c = (S_{pp} + S_p r_p + S_c r_c) N^2 / R \tag{1}$$

其中 S_{pp} 是预准备消息的大小，S_p 是准备消息的大小，S_c 是确认消息的大小，r_p，r_c 为准备消息和确认消息的重试次数。R 是两个验证者节点之间最慢的通信通道的带宽。尽管 S_p 和 S_c 是不变的常量，但预准备消息会搭载块 b，因此 S_{pp} 通常取决于块大小。由于 R 通常是一个常数，取决于连接验证器节点的基础结构，因此可以通过调整块的大小和消息的重试次数来缩短等待时间。

块的大小是其中事务的大小加上块头 s_H 的大小之和(常数)。在所提出的取证模型中，s_H 是一个常数。区块中的实际交易数量和类型取决于许多因素，包括区块周期 T 以及最终在给定时间段内发送的特定交易集合等。因此，不同的块通常具有不同的大小，但是除非网络状态极差或重试次数过多，共识速度均可以满足处理需要。

3.2.2 区块链增长率

由于每个块都有固定大小的标头，因此创建的块数越大，与区块链中的交易相比，块标头占用的空间越大，即空间开销越大。区块头的大小开销，即在任何时间 t 的块标头的总大小可由式(2)得到：

$$OH(t) = s_H \frac{t}{T} \tag{2}$$

值得注意的是，该值仅取决于时间 t 链中的块数，而不是交易次数。

假设 $I(t)$ 是时间 t 包含在区块链中的交易集，则时间 t 的区块链总大小的计算公式如式(3)所示。

$$S_m(t) = s_g + overhead_m(t) + \sum_{tx \in I(t)} s(tx) \tag{3}$$

其中 s_g 是创世块的大小。

因此，在时间间隔 $[t_1, t_2]$ 上的增长率为 $S_m(t_2) - S_m(t_1)$，计算公式如式(4)所示。

$$G(t_1; t_2) = s_H \frac{t_2 - t_1}{T} + \sum_{tx \in I(t_1; t_2)} s(tx) \tag{4}$$

显然，区块链随着时间增长的速度主要取决于交易率。影响增长率的另一个因素是区块周期 T，此参数会影响块头开销，从而影响等式 4 的第一项。假设每年创建和删除新的证据 n 次，即使存在大量的证据收集(每年 100 万次)和传输(每年 1000 万次)，每年的增长率也为 GB 级别，考虑到当今存储设备的容量是可以接受的。

3.2.3 与现有电子取证模型的综合对比

本节通过与现有基于区块链的电子取证模型以及传统方式的电子取证模型进行对比来分析所提模型的具体表现，具体对比情况如表 1 所示。

通过比较可知，基于区块链的取证模型由于摆脱了中心机构的制约，因此具有更好的安全性和防篡改特性，但由于以往取证模型多采用了基于拜占庭容错的共识机制，在可扩张性和吞吐性能方面的表现不佳。本文提出的方案将委托权益证明与传统的基于拜占庭机制结合，在保留区块链取证模

型相较传统取证模型优势的基础上，增强了可扩展性和单位时间的吞吐量，使其能够更好地满足高并发场景的需要。

表 1　各电子取证模型性能对比

Tab. 1　Performance comparison of forensics models

方案名称	去中心性	可扩展性	防窜改性	存储安全性	单位时间吞吐量
本文模型	高	高	高	高	高
基于拜占庭容错的电子取证模型	高	低	高	高	低
传统电子取证模型	无	高	弱	低	高

4　结束语

在当前的数字取证调查中，维护数据完整性的工作是由相关中心机构独立进行的。这具有足够的程序便利性，但是如果恶意攻击者攻击机构，则可能会破坏潜在证据的完整性。凭借区块链技术的去中心化防窜改特性，可以使电子证据摆脱中心化机构的制约，提高存证效率和可信性。现有基于区块链的电子取证模型工作多采用了考虑拜占庭故障的实用拜占庭容错算法及其改进算法，但诸如实用拜占庭容错算法之类的强一致性算法复杂度高且去中心化程度不足，较为适合节点数量相对较少的应用场景。本文提出了一种基于委托权益证明-实用拜占庭容错的链上链下结合的区块链电子取证模型，通过委托权益证明推选出的节点通过实用拜占庭容错机制实现同步，将电子证据数据采用链上链下结合的方式进行存储，以提高现有基于区块链的取证模型的可扩展性和可用性。通过对所提模型进行安全性和效率分析，在保证网络安全的前提下，整个网络的能耗进一步降低，在各种可能的自然网络中断情况下，所提模型十分健壮。下一步的工作重点在于在真实应用场景中部署，在实际情况中进一步优化共识算法，提高吞吐率和交易速率，使模型能够适应更大规模的数据使用。

参考文献：

[1] 刘品新. 论电子证据的定位——基于中国现行证据法律的思辨 [J]. 法商研究, 2002 (4): 37-44. (Liu Pinxin. Discuss of the positioning of electronic evidence—based on the current evidence law of China [J]. Studies in Law and Business, 2002 (4): 37-44)

[2] 常怡, 王健. 论电子证据的独立地位 [J]. 法学论坛, 2004, 19 (1): 66-74. (Chang Yi, Wang Jian. On the independent status of electronic evidence [J]. Legal Forum, 2004, 19 (1): 66-74)

[3] 许康定. 电子证据基本问题分析 [J]. 法学评论, 2002 (3): 94-99. (Xu Kangding. Analysis of basic problems of electronic evidence [J]. Law Review, 2002 (3): 94-99)

[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. 2008. https://bitcoin. org/bitcoin. pdf

[5] 王发明, 朱美娟. 国内区块链研究热点的文献计量分析 [J]. 情报杂志, 2017 (12): 73-78. (Wang Chuang, Zhu Meijuan. Bibliometric analysis on the research hotspots of blockchain in China [J]. Journal of Intelligence, 2017 (12): 73-78)

[6] 商琦, 陈洪梅. 区块链技术创新态势专利情报实证 [J]. 情报杂志, 2019, 38 (04): 27-32. (Shang Qi, Chen Hongmei. Empirical analysis of the patent intelligence on the innovation Status of blockchain technology [J]. Journal of Intelligence, 2019, 38 (04): 27-32)

[7] 赵丹, 王晰巍, 韩洁平, 等. 区块链环境下的网络舆情信息传播特征及规律研究 [J]. 情报杂志, 2018 (9): 127-133. (Zhao Dan, Wang Xiwei, Han Jieping, *et al.* Research on the propagation characteristics and rules of network public opinion information in blockchain environment [J]. Journal of Intelligence, 2018 (9): 127-133)

[8] 涂奔, 张李义, 陈晶. 一种基于私有区块链的信息保护预测模型研究 [J]. 情报理论与实践, 2017 (10): 110-115. (Tu Ben, Zhang Liyi, Chen Jing. Research on the prediction model of information protection based on private blockchain [J]. Information Theory and Practice, 2017 (10): 110-115)

[9] 孔繁超. 基于区块链的开放获取资源建设与管理 [J]. 情报理论与实践, 2019, 42 (05): 157-162. (Kong Fanchao. Construction and management of open access resources based on blockchain [J]. Information Studies: Theory & Application, 2019, 42 (05): 157-162)

[10] 汪闽燕. 电子证据的形成与真实性认定 [J]. 法学, 2017 (6): 185-194. (Wang Minyan. The formation and authenticity of electronic evidence [J]. Law Science, 2017 (6): 185-194)

[11] 褚福民. 电子证据真实性的三个层面——以刑事诉讼为例的分析 [J]. 法学研究, 2018 (4): 121-138. (Chu Fumin. Three aspects of the authenticity of electronic evidence-an analysis of criminal proceedings as an example [J]. Chinese Journal of Law, 2018 (4): 121-138)

[12] 刘品新. 印证与概率: 电子证据的客观化采信 [J]. 环球法律评论, 2017 (4): 109-127. (Liu Pinxin. Confirmation and probability: objective acceptance of electronic evidence [J]. Global Law Review, 2017 (4): 109-127)

[13] 周新. 刑事电子证据认证规范之研究 [J]. 法学评论, 2017 (6): 158-166. (Zhou Xin. Research on the certification norms of criminal electronic evidence [J]. Law Review, 2017 (6): 158-166)

[14] 黄晓芳, 徐蕾, 杨茜. 一种区块链的云计算电子取证模型 [J]. 北京邮电大学学报, 2017, 40 (6): 120-124. (Huang Xiaofang, Xu Lei, Yang Qian. Blockchain model of cloud forensics [J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40 (6): 120-124)

[15] 侯义斌, 梁勋, 占小瑜. 基于区块链的电子证据系统架构模型 [J]. 计算机科学, 2018, 45 (6): 348-351. (Hou Yibin, Liang Xun, Zhan Xiaoyu. Blockchain based architecture model of electronic evidence system [J]. Computer Science, 2018, 45 (6): 348-351)

[16] Cebe M, Erdin E, Akkaya K, *et al.* Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles [J]. IEEE Communications Magazine, 2018, 56 (10): 50-57.

[17] Bonomi S, Casini M, Ciccotelli C. B-coc: A blockchain-based chain of custody for evidences management in digital forensics [J]. ArXiv Preprint ArXiv: 1807. 10359, 2018.

[18] Ryu J H, Sharma P K, Jo J H, *et al.* A blockchain-based decentralized efficient investigation framework for IoT digital forensics [J]. The Journal of Supercomputing, 2019, 75 (8): 4372-4387.